ICS 03.060
A11

JR

# 中 华 人 民 共 和 国 金 融 行 业 标 准

XX/T XXXXX—XXXX

# 证券期货业信息技术服务连续性管理指南

Information technology service continuity management guidance for securities and futures industry

点击此处添加与国际标准一致性程度的标识

（送审稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　发 布

# 目　　次

# 前　言

本标准依据GB/T 1.1—2009给出的规则起草。

本标准由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国证券监督管理委员会、上海期货交易所、上海证券交易所、深圳证券交易所、大连商品交易所、海通证券股份有限公司、安信证券股份有限公司、兴业证券股份有限公司、国泰君安证券股份有限公司、中原证券股份有限公司、西南证券股份有限公司、招商证券股份有限公司、方正中期期货有限公司、倍特期货有限公司、汇添富基金管理股份有限公司、中国信息安全认证中心、中国标准化研究院。

本标准主要起草人：张野、刘铁斌、支晓繁、卫飞、周云晖、王东明、李向东、陈炜、刘宁、金庆风、马赟琪、游沁沁、王洪涛、王东、许彦冰、梁德汉、聂君、王玥、吴佳伟、史哲、袁维举、李鲁川、李华威、杨潇、黄锦川、刘卓彪、杨飞、邓列军、王方舟、尤其、魏立茹、秦挺鑫、孙伟、薛利、况家兴、陆志坚、刘宁、卢剑雄、张德龙、邵瑾、杨景涛、杨文纶。

# 引　言

证券期货业的平稳运行高度依赖于行业机构信息技术服务的连续性。信息技术服务连续性管理，不仅关系到证券期货市场的稳定和健康发展，还关系到国家金融安全和社会稳定，同时，对于保护投资者合法权益也有积极意义。

为了引导行业机构正确认识信息技术服务连续性管理的重要性，强化信息技术服务连续性管理的组织保障，规范信息技术服务连续性管理的实施过程，提升行业机构内相关部门对信息技术服务连续性管理的参与度，协调推动行业机构与供应商的沟通与配合，制定本指南。

行业机构可依据本指南开展信息技术服务连续性管理工作。

# 证券期货业信息技术服务连续性管理指南

## 1 范围

本标准为证券期货行业机构开展信息技术服务连续性管理工作提供了指南，说明了证券期货行业机构开展信息技术服务连续性管理的程序和措施。行业机构依据本指南，对因下述原因导致的信息技术服务中断事件进行事前、事中和事后管理，包括：

——技术故障：信息系统故障、基础设施故障等；

——外部服务中断：停电、停水、通信中断等；

——人为破坏：操作失误、网络攻击、恐怖袭击等；

——自然灾害：火灾、台风、海啸、地震等。

行业机构通过信息技术服务连续性管理：

a) 提升信息技术服务连续性管理水平，预防信息技术服务中断事件发生；

b) 信息技术服务中断事件发生后，可依照信息技术服务连续性计划进行处置，控制中断事件的负面影响，在可接受的时间范围内将信息技术服务恢复到可接受的水平；

c) 对于已发生的信息技术服务中断事件，总结经验教训，改进管理过程，避免类似事件再次发生。

本标准适用于证券期货行业机构（以下简称行业机构），包括承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其下属机构(以下简称核心机构)，以及证券公司、基金管理公司、期货公司、证券期货服务机构等证券期货经营机构（以下简称经营机构）。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 30146-2013 公共安全 业务连续性管理体系 要求

JR/T 0059-2010 证券期货经营机构信息系统备份能力标准

## 3 术语和定义

GB/T 30146-2013界定的以及下列术语和定义适用于本文件。

3.1

**业务影响分析 business impact analysis**

分析活动和业务中断可能带来的影响的过程。

[GB/T 30146-2013，定义3.8]

3.2

**信息技术服务连续性管理 information technology service continuity management**

识别行业机构在提供信息技术服务过程中面临的潜在威胁以及减少这些威胁一旦发生可能对行业机构整体业务运行带来的影响的一套管理过程。该过程为行业机构建立有效应对威胁的自我恢复能力提供了框架，以保护行业机构自身和关键相关方的利益、声誉、社会稳定的活动。

3.3

**信息技术服务连续性计划 information technology service continuity plan**

用于指导行业机构在信息技术服务中断事件发生时进行响应、恢复、重新开始和还原到预先确定的服务运行水平的形成文件的程序。

3.4

**信息技术服务中断事件 information technology service interruption**

可预期或不可预期的、导致非计划的、与行业机构所期望交付的信息技术服务相背离的、将导致中断、损失、紧急状况或危机的情况。

3.5

**恢复时间目标 recovery time objective; RTO**

中断事件发生后到下列活动完成之前的时间段。

——产品或服务必须恢复，或

——活动必须恢复，或

——资源必须恢复。

注：对于产品、服务和活动，恢复时间目标必须小于组织不能接受的导致产品/服务停止供应、活动无法执行等负面影响所需的时间。

[GB/T 30146-2013，定义3.44]

3.6

**恢复点目标 recovery point objective; RPO**

为使活动能够恢复进行，而必须将该活动所用的信息恢复到某时间点。

[GB/T 30146-2013，定义3.45]

3.7

**风险评估 risk assessment**

风险识别、风险分析和风险评价的整个过程。

[GB/T 30146-2013，定义3.50]

## 4 组织架构

### 4.1 概述

行业机构明确信息技术服务连续性管理的组织架构，确定各层级人员在信息技术服务连续性管理过程中的职责和分工。

信息技术服务中断事件发生后，行业机构启用应急处置组织架构。

### 4.2 高级管理层

行业机构高级管理层负责领导本机构的信息技术服务连续性管理工作，主要职责包括：

a) 建立信息技术服务连续性管理组织架构，明确公司、部门及分支机构在信息技术服务连续性管理方面的职责、工作流程；

b) 审核并批准信息技术服务连续性管理相关制度和信息技术服务连续性管理各项任务的输出文档，如实施计划、连续性评估报告等；

c) 监督各层级人员的履职情况，定期听取信息技术服务连续性管理委员会的工作汇报，建立相应的绩效考核、奖惩机制。

### 4.3 信息技术服务连续性管理委员会

行业机构设立信息技术服务连续性管理委员会，或授权机构内已存在的相关委员会承担信息技术服务连续性管理委员会的职能。

信息技术服务连续性管理委员会由高级管理层的一名成员直接领导，并包含技术、风险管理、业务、公共关系、后勤、安保等与信息技术服务连续性管理有关的部门负责人。

信息技术服务连续性管理委员会的职责主要包括：

a) 承担高级管理层授权的工作，落实高级管理层的各项决策；

b) 推动、协调、督促相关部门开展信息技术服务连续性管理工作；

c) 审核信息技术服务连续性管理各项任务的输出文档。

信息技术服务连续性管理委员会下设信息技术服务连续性管理工作组，负责落实和协调信息技术服务连续性管理委员会安排的各项任务。

### 4.4 机构内各部门

行业机构内各部门在高级管理层和信息技术服务连续性管理委员会领导下，分工协作，完成信息技术服务连续性管理各项任务。

行业机构指定信息技术服务连续性管理牵头部门，负责牵头并组织相关部门开展信息技术服务连续性管理各项工作。

机构内其他部门配合牵头部门，完成与信息技术服务连续性管理有关的各项工作。

### 4.5 应急处置组织架构

行业机构应急处置组织架构包括：

a) 应急处置领导小组：主要由高级管理层成员组成，负责决策中断事件处置过程中的重大事项。职责主要包括：
   1) 批准中断事件处置方案；
   2) 批准向监管机构报告内容；
   3) 批准对外公告内容等；

b) 应急处置工作小组：主要由信息技术服务连续性管理相关部门负责人组成，负责落实领导小组的各项决策。职责主要包括：
   1) 向领导小组汇报事件进展和处置情况；
   2) 制定中断事件处置方案；
   3) 部门间的沟通和协调等；

c) 各部门负责实施中断事件处置工作。

### 4.6 管理制度

行业机构制定信息技术服务连续性管理制度，或在相关制度中说明与信息技术服务连续性管理有关的要求，包括且不限于：

——高级管理层在信息技术服务连续性管理中承担的职责；

——信息技术服务连续性管理委员会的组成人员和职责；

——应急处置领导小组和工作小组的组成人员和职责；

——相关部门和人员的职责；

——其他需要在制度中说明的事项。

## 5 策划

### 5.1 概述

行业机构策划信息技术服务连续性管理过程，依据信息技术服务连续性管理的指导原则，明确各项任务并制定实施计划。

### 5.2 指导原则

行业机构开展信息技术服务连续性管理的指导原则包括：

——将信息技术服务连续性管理作为行业机构业务连续性管理的基本组成部分，并纳入行业机构全面风险管理体系中；

——提升员工的业务连续性管理意识，将信息技术服务连续性管理融入到行业机构日常管理工作中；

——提供必要的资金和人员支持，确保信息技术服务连续性管理水平符合业务发展的要求；

——组织行业机构内相关部门共同参与，协同配合；

——在突发事件处置过程中优先保障人员的生命安全。

### 5.3 任务

行业机构开展信息技术服务连续性管理的任务主要包括：

a) 制定信息技术服务连续性管理实施计划；
b) 开展业务影响分析和信息技术服务连续性风险评估；
c) 制定信息技术服务连续性策略，准备连续性管理所需资源；
d) 制定和维护信息技术服务连续性计划；
e) 开展信息技术服务连续性管理培训和演练；
f) 开展信息技术服务连续性评估和改进。

### 5.4 实施计划

行业机构编制书面文档说明信息技术服务连续性管理的实施计划。实施计划的内容主要包括：

a) 实施计划的目的和范围；
b) 制定实施计划的部门、人员和职责分工；
c) 计划开展的各项任务的名称、时间要求、责任部门、配合部门等；
d) 每项任务的工作计划，包括参与部门、工作程序、所需资源、输出文档等；
e) 总结和建议。

## 6 业务影响分析

### 6.1 概述

行业机构定期开展业务影响分析，识别业务之间的依赖关系，评估业务中断影响，明确业务的重要性程度和恢复的优先顺序，并据此确定信息技术服务恢复目标及所需资源。

### 6.2 识别和分析业务

行业机构开展以下工作：

a) 识别与经营有关的各项业务，分析业务之间的关联关系，以及业务与信息技术服务的依赖关系；
b) 评估业务中断对机构带来的负面影响，评估内容包括：
   1) 业务中断可能造成的直接和间接经济损失，包括资产损失、赔偿、行政处罚等；
   2) 业务中断可能造成的非经济影响，包括社会声誉影响、信用影响等；
   3) 随着业务中断时间的延长，中断事件带来的各类负面影响的变化情况。
c) 依据业务中断影响评估结果，确定业务的重要性程度，以及业务恢复的优先级顺序。

### 6.3 信息技术服务恢复目标

行业机构基于业务的重要性程度、业务恢复的优先级顺序以及业务与信息技术服务的依赖关系，依据《证券期货经营机构信息系统备份能力标准》，设定信息技术服务恢复时间要求（RTO）和恢复点要求（RPO），以及信息技术服务恢复的优先级顺序。

行业机构识别恢复信息技术服务所需的最低资源保障。与信息技术服务有关的资源包括信息系统、数据、基础设施、办公场所、通讯设施、人员、供应商、文档等。

### 6.4 业务影响分析报告

行业机构编制业务影响分析报告，说明业务影响分析的实施过程和结果。业务影响分析报告的内容主要包括：

a) 业务影响分析的目的和范围；
b) 参与业务影响分析的部门、人员和职责分工；
c) 业务影响分析的实施过程；
d) 业务影响分析结论，包括信息技术服务恢复时间目标（RTO）和恢复点目标（RPO），信息技术服务恢复的优先级顺序等；
e) 总结和建议。

## 7 连续性风险评估

### 7.1 概述

行业机构定期开展面向信息技术服务连续性的风险评估，对信息技术服务及其依赖资源的中断风险进行识别、分析和评估，并根据风险评估结果制定风险控制策略。

### 7.2 风险识别和评估

行业机构开展以下工作：

a) 识别风险：识别机构的信息技术服务和支持这些服务的资源。风险可能来自于：
   1) 特定的威胁，可被描述为在一些点上中断服务或资源的事态或活动（例如火灾、水灾、电力中断、硬件故障等）；
   2) 中断事件，可产生于资源脆弱性（如单点故障、缺乏后备电力、人员配备水平不足等）。
b) 风险评估：分析风险可导致的后果和风险发生的可能性，评估哪些与中断有关的风险需要处置，重点关注高优先级的信息技术服务所要求的资源；
c) 处置识别：识别可实现信息技术服务连续性目标并符合组织风险偏好的处置措施。

### 7.3 连续性风险评估报告

行业机构编制信息技术服务连续性风险评估报告，说明连续性风险评估的过程和结果。风险评估报告的内容主要包括：

a) 风险评估的目的和范围；
b) 参与风险评估的部门、人员和分工；
c) 风险评估的实施过程；
d) 风险评估结果，包括风险列表、风险控制措施和残余风险等；
e) 总结和建议。

## 8 连续性策略

### 8.1 概述

行业机构定期制定或完善本机构的信息技术服务连续性策略。根据业务影响分析和连续性风险评估结果，制定或更新连续性策略内容，对策略的可行性进行评估。

### 8.2 制定策略

信息技术服务连续性策略包括且不限于：

——信息技术服务中断事件决策和授权策略；
——信息系统应急处置和恢复策略；
——信息系统灾备建设策略；
——重要岗位人员备份策略；
——信息技术服务风险控制策略；
——危机沟通策略等。

行业机构宜：

——接受来自监管机构、公共服务机构、供应商、业务关联机构等发布的预警信息，并及时采取措施预防可能发生的信息技术服务中断事件；
——确保信息技术服务相关供应商的业务连续性，尤其是如不能交付服务将立即导致信息技术服务中断的供应商。

行业机构可根据需要，与相关机构签订协议，以便在信息技术服务中断事件发生后可获取所需的资源或服务。

### 8.3 评估策略

行业机构对连续性策略进行评估，包括：

a) 评估策略实施的可行性；
b) 评估新策略是否会引入额外的风险；
c) 评估策略实施的成本和收益。

### 8.4 连续性策略报告

行业机构编制信息技术服务连续性策略报告，说明连续性策略的制定过程和结果。连续性策略报告的内容主要包括：

a) 连续性策略的目的和范围；
b) 参与制定连续性策略的部门、人员和职责分工；
c) 策略制定过程和结果。策略结果包括拟采用方法或措施、所需资源、责任部门、时间要求等；

d) 总结和建议。

## 9 资源准备

### 9.1 概述

行业机构根据业务影响分析和信息技术服务连续性风险评估结果，在信息技术服务连续性策略指导下，建设信息技术服务连续性管理所需资源并定期维护，保障信息技术服务连续性计划顺利执行。

行业机构将信息技术服务连续性作为信息系统和基础设施建设的基本需求，并在人员配置过程中考虑到信息技术服务连续性管理的需求。

### 9.2 人员

行业机构识别适当的措施来维护、扩充核心技能和知识的可用性，以应对事件导致员工可用性减少的事态。这些措施主要包括：

——为人员提供信息技术服务连续性管理培训和专业技能培训；

——为关键岗位准备备份人员；

——制定人员继任计划；

——分散核心能力以减少事件的影响；

——建立保留知识和经验的文档管理过程。

### 9.3 信息和数据

行业机构保护对信息技术服务正常运行所需的信息和数据，并确保这些信息和数据的恢复能够满足机构设定的信息技术服务恢复目标要求。

### 9.4 场所和设施

行业机构建设和维护信息技术服务连续性管理所需的场所和设施，主要包括：

——灾备数据中心及配套基础设施；

——应急指挥中心及配套通讯设施；

——消防、应急照明等设施；

——应对机构所在地可能发生的自然灾害（如水灾等）所需的防灾减灾设施；

——通勤交通工具等。

### 9.5 信息系统

行业机构建设可满足信息技术服务连续性需求的信息系统。信息系统的数据备份能力和故障应对能力符合信息技术服务恢复目标要求。

行业机构考虑以下事项：

——采用高可用的信息系统架构；

——采用自动故障切换方式替代人工干预；

——提供额外的通信线路；

——管控信息系统的变更过程；

——强化信息系统安全管理；

——定期对信息系统备份能力进行测试。

### 9.6 供应商

行业机构确保其信息技术服务所选关键设备供应商具备有效的业务连续性管理措施。可采取的措施包括：

——评估供应商的业务连续性能力，尤其应关注如不能提供服务或产品将立即导致信息技术服务中断的供应商；

——在标书和合同中要求与信息技术服务连续性有关的技术参数和服务要求；

——定期审核供应商的业务连续性计划。

### 9.7 操作手册

行业机构编制信息系统、基础设施、通讯设施、防灾减灾设施等信息技术服务相关资源的操作手册，供信息技术服务中断事件处置过程中参考和使用。

操作手册包括资源的功能、使用方法、配置信息、管理员信息、常见故障的解决方法等内容。

### 9.8 应急沟通

行业机构提供应急联系途径，接收来自客户或其他相关方的信息技术服务中断事件投诉或通知信息，对这些信息进行记录，通知相关部门进行核实和处置。

行业机构记录监管机构、供应商、公共服务机构、媒体等相关方联系方式并定期更新。

### 9.9 连续性资源报告

行业机构编制连续性资源报告，说明信息技术服务连续性策略所需资源准备情况。资源报告的内容主要包括：

a) 资源报告的目的和范围；
b) 参与资源准备的部门、人员和职责分工；
c) 资源准备过程和结果；
d) 总结和建议。

## 10 连续性程序

### 10.1 概述

行业机构依据信息技术服务风险评估和业务影响分析结果，在信息技术服务连续性策略指导下，建立信息技术服务连续性程序，编制信息技术服务连续性计划，确保信息技术服务中断事件能够得到及时响应和处置。

信息技术服务连续性计划可用于指导行业机构在信息技术服务中断事件发生时进行响应、处置和恢复。机构内与信息技术服务连续性管理有关的预案、沟通和决策程序、信息系统恢复程序等可作为信息技术服务连续性计划的组成部分。

行业机构依据自身实际情况，明确纳入信息技术服务连续性计划范畴内的预案或程序。根据需要完善现有程序或设立新的程序，确保信息技术服务连续性计划的内容能覆盖信息技术服务中断事件的发现、响应、恢复等主要环节，并可指导信息技术服务中断事件处置过程有序实施。

信息技术服务连续性程序宜考虑灵活应对非预期的威胁和不断变化的内部和外部环境，并通过实施适当的缓解策略，最大限度地减轻中断事件所造成的后果。

### 10.2 发现事件

行业机构采取措施发现信息技术服务连续性中断事件，并判断是否启动正式响应：

a) 采用自动化监测、人工巡检等方式发现事件；
b) 接受来自外部的预警、投诉、通知等；
c) 对事件进行核实，对发现的情况进行初步处置；
d) 评估中断事件的性质和程度，或其可能造成的影响；
e) 判断是否应启动正式响应。

### 10.3 响应事件

行业机构启动信息技术服务中断事件响应机制后，采取的措施包括：
a) 启用信息技术服务中断事件应急处置组织架构；
b) 评估和选择事件处置策略，包括是否需要进行灾备系统切换；
c) 根据事件处置策略进行事件处置，记录事件处置过程；
d) 向监管机构报告事件情况；
e) 持续跟踪外部相关方的反应，包括客户、媒体等，并依据危机沟通策略进行沟通。

### 10.4 恢复正常运行

行业机构制定将信息技术服务从中断事件发生后所采取的临时性措施恢复到正常运行状态的程序，包括：
a) 选择恢复到正常运行的方案；
b) 确定信息技术服务已恢复到正常水平；
c) 核对重要业务数据，追补丢失数据；
d) 进行测试，确保信息技术服务的可靠性、有效性。

### 10.5 总结事件处置过程

行业机构在信息技术服务连续性中断事件应急处置结束、服务恢复正常运行后，对事件处置过程进行总结。

事件总结报告内容主要包括：
a) 事件概况，包括事件的发生经过、事件影响范围和损失；
b) 应急处置过程，包括事件向监管机构报告的过程、采取的措施及效果；
c) 事件发生的主要原因分析、结论；
d) 事件后续预防和改进措施。

行业机构以文件形式记录信息技术服务中断事件处置过程中采取的措施、决策、报告等相关重要信息并归档保存。

### 10.6 连续性计划

信息技术服务连续性计划是包含指导行业机构在信息技术服务中断事件发生时进行处置和恢复的一个或多个书面程序或预案的总称。这些程序或预案的内容主要包括：
a) 目的和范围；
b) 参与部门、人员和职责分工；
c) 启动准则和程序；
d) 实施程序，包括沟通的要求和程序；
e) 资源要求。

行业机构可通过演练、评估等方式确保信息技术服务连续性计划的有效性。

# 11 培训

## 11.1 概述

行业机构定期开展信息技术服务连续性培训，提升人员的业务连续性意识和技能，逐步建立业务连续性管理的企业文化。

行业机构将信息技术服务连续性管理培训纳入机构的人员培训体系。

行业机构在开展业务影响分析、连续性风险评估、演练等任务前安排相关培训，说明任务实施方法和注意事项。

## 11.2 培训内容

信息技术服务连续性培训的内容包括且不限于：

——信息技术服务连续性管理制度；

——国家法律法规，行业监管要求；

——信息技术服务连续性管理实施程序和方法；

——信息技术服务连续性管理案例；

——外部沟通方法和要求，包括与客户、媒体沟通等。

## 11.3 培训报告

行业机构编制信息技术服务连续性管理培训报告。培训报告的内容主要包括：

a) 连续性培训的目的和范围；

b) 组织和参与培训的部门、人员和职责分工；

c) 培训过程和结果；

d) 总结和建议。

# 12 演练

## 12.1 概述

行业机构定期开展信息技术服务连续性演练，检验信息技术服务连续性计划的有效性和信息技术服务连续性资源的可用性，提升信息技术服务中断事件的处置能力。

行业机构的信息技术服务连续性演练以发现信息技术服务连续性计划中存在的问题作为演练的目的。

行业机构可根据需要，通知供应商、业务相关机构等参加演练。

行业机构确保演练过程不对机构的业务运营带来风险。

## 12.2 演练流程

行业机构依照以下流程开展演练：

a) 演练准备，包括制定计划、设计方案、方案评审、演练培训、演练保障等；

b) 演练实施，包括系统准备、演练启动、演练执行、演练记录、演练结束和系统恢复等；

c) 演练总结，包括演练评估、文件归档和备案、考核与奖惩等；

d) 演练成果运用，包括改进信息技术服务连续性计划、改进管理过程、培训等。

行业机构设计满足演练目标的演练场景，可以利用风险评估中确定的威胁或其他适当的事件。

演练的设计和执行完成以下一种或几种任务：

——验证信息技术服务恢复时间目标（RTO）和恢复点目标（RPO）是可实现的；
——提高对于信息技术服务连续性计划的内容及其使用的理解；
——提高对信息技术服务中断事件进行处置的信心；
——评估信息技术服务连续性策略的效用及其适用性；
——评估已有的能力和配备的资源是否充分；
——识别在处置信息技术服务中断事件过程中，是否存在此前没有考虑到的情况；
——识别所编写的信息技术服务连续性计划及其贯彻执行中存在的不足之处。

### 12.3 演练报告

行业机构编制演练报告，说明信息技术服务连续性演练的实施情况。演练报告的内容主要包括：
a) 演练的目的和范围；
b) 参与演练的部门、人员和职责分工；
c) 场景设置和演练形式；
d) 演练过程和结果；
e) 总结和建议。

## 13 连续性评估

### 13.1 概述

行业机构定期开展信息技术服务连续性评估，检查机构对行业监管要求及其自身信息技术服务连续性管理制度的符合性，评价信息技术服务连续性计划的有效性，评估信息技术服务连续性管理过程的合理性，并提出改进建议。

行业机构可依据自身情况，设定符合机构需求的绩效指标，包括定量和定性的测量指标，作为评价本机构信息技术服务连续性水平的参考依据。

### 13.2 评估内容

信息技术服务连续性评估的内容包括且不限于：
——信息技术服务连续性管理过程是否满足相关的法律法规和行业监管要求；
——信息技术服务连续性管理能力是否能够应对机构面临的主要风险；
——信息技术服务连续性管理制度是否落实，各部门的职责分工是否合理明确；
——信息技术服务连续性管理实施计划是否按期完成，各项任务实施结果是否符合预期；
——业务影响分析得到的信息技术服务 RTO 和 RPO 是否合理；
——信息技术服务风险评估发现的各类风险是否得到控制或持续关注；
——信息技术服务连续性策略是否落实，是否取得预期效果；
——信息技术服务连续性管理所需资源是否得到保障，已建成资源是否得到有效维护；
——信息技术服务连续性演练过程的合理性和充分性，演练是否能对信息技术服务 RTO 和 RPO 进行检验；
——信息技术服务连续性计划在真实场景中是否有效；
——如发生信息技术服务中断事件，事件处置过程是否合理。

### 13.3 连续性评估报告

行业机构编制信息技术服务连续性评估报告。评估报告的内容主要包括：

a) 连续性评估的目的和范围；
b) 参与评估的部门、人员和职责分工；
c) 评估过程和结果；
d) 总结和建议。

## 14 改进

### 14.1 概述

行业机构对信息技术服务连续性管理过程进行改进，改进对象包括制度、管理程序、方法、文档等。

信息技术服务连续性改进的问题线索来源于信息技术服务连续性评估和其他在连续性管理实施过程中发现的问题。

### 14.2 改进过程

改进信息技术服务连续性管理的过程主要包括：

a) 识别连续性管理存在的问题；
b) 识别当前的工作过程和控制措施；
c) 确定需要采取的改进措施，制定改进计划。改进计划包括责任部门、配合部门、措施、时间要求、所需资源等；
d) 根据改进计划，实施改进措施。

### 14.3 改进报告

行业机构制定信息技术服务连续性管理改进报告，说明改进工作的实施过程和结果。改进报告的内容主要包括：

a) 改进的目的和范围；
b) 参与改进的部门、人员和职责分工；
c) 改进过程和结果；
d) 总结和建议。

# 参 考 文 献

[1] GB/T 31595-2015 公共安全 业务连续性管理体系 指南
[2] JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求
[3] JR/T 0067-2011 证券期货业信息系统安全等级保护测评要求
[4] JR/T 0071-2012 金融行业信息系统信息安全等级保护实施指引
[5] JR/T 0072-2012 金融行业信息系统信息安全等级保护测评指南
[6] JR/T 0073-2012 金融行业信息安全等级保护测评服务安全指引
[7] JR/T 0099-2012 证券期货业信息系统运维管理规范